#2
6/28/01

Docket No. 826.1701

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Takayuki HASEBE, et al.

Serial No.: To be Assigned

Filed: March 14, 2001

Group Art Unit: To be Assigned

Examiner: To be Assigned

For: **DATE-AND-TIME MANAGEMENT DEVICE AND SIGNATURE GENERATION APPARATUS WITH DATE-AND-TIME MANAGEMENT FUNCTION**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-293366
Filed: September 27, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

Date: 3/14/01

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:　２０００年　９月２７日

出願番号
Application Number:　特願２０００－２９３３６６

出願人
Applicant (s):　富士通株式会社

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office　及川耕造

出証番号　出証特２０００－３１０５８８１

【書類名】　特許願
【整理番号】　0051524
【提出日】　平成12年 9月27日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明の名称】　日時管理装置および日時管理機能内蔵署名作成装置
【請求項の数】　20
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　長谷部　高行
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小谷　誠剛
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100074099
【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ
【弁理士】
【氏名又は名称】　大菅　義之
【電話番号】　03-3238-0031
【選任した代理人】
【識別番号】　100067987
【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３
【弁理士】
【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　日時管理装置および日時管理機能内蔵署名作成装置

【特許請求の範囲】

【請求項１】　複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理装置において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には、該あらかじめ定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段とを備えることを特徴とする日時管理装置。

【請求項２】　階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理装置において、

前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けた後には、該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段とを備えることを特徴とする日時管理装置。

【請求項３】　前記日時管理者側に管理者用の日時管理装置を備え、

該管理者用日時管理装置が、自装置が管理する日時の複写の要求を前記日時設定要求として前記日時設定要求受付手段に与える日時設定要求手段を備えることを特徴とする請求項１、または２記載の日時管理装置。

【請求項４】　前記日時設定要求手段が、前記日時設定要求を受け付けた日時管理装置から送られた非再現性の情報と、前記管理者用日時管理装置が管理する日時とを用いて、前記日時の複写のためのデータを生成する日時複写データ生成手段を更に備えることを特徴とする請求項３記載の日時管理装置。

【請求項５】　前記日時複写データ生成手段が、前記非再現性の情報と前記管理する日時の情報とを暗号化して、日時複写のためのデータを生成することを

特徴とする請求項４記載の日時管理装置。

【請求項６】　前記日時複写データ生成手段が、前記非再現性の情報と前記管理する日時の情報とを暗号化した結果から署名を作成し、該非再現性の情報、管理する日時、および署名を合わせて日時複写のためのデータを生成することを特徴とする請求項４記載の日時管理装置。

【請求項７】　前記日時管理装置の出荷元に更に日時管理装置を備えると共に、

該出荷元の日時管理装置が、前記管理者用日時管理装置の出荷時に、該管理者用日時管理装置に日時を設定する日時設定手段を備えることを特徴とする請求項３記載の日時管理装置。

【請求項８】　複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理機能を内蔵する署名作成装置において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には該あらかじめ定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段と、

該時計手段が示す日時の情報を用いて、入力される署名対象データに対する署名を作成する署名作成手段とを備えることを特徴とする日時管理機能内蔵署名作成装置。

【請求項９】　階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理機能を内蔵する署名作成装置において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には該あらかじめ定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けた日時設定要求に対応して動作する時計手段と、

該時計手段が示す日時の情報を用いて、入力される署名対象データに対する署名を作成する署名作成手段とを備えることを特徴とする日時管理機能内蔵署名作成装置。

【請求項１０】　前記日時管理機能内蔵署名作成装置において、

前記時計手段の動作停止が検出された時、前記署名作成手段による署名作成を停止させる署名停止手段を更に備えることを特徴とする請求項８、または９記載の日時管理機能内蔵署名作成装置。

【請求項１１】　前記日時管理機能内蔵署名作成装置が、前記署名作成の機能と異なる1 つ以上の他の機能を更に備えると共に、

前記時計手段の動作停止が検出された時、該署名作成の機能と異なる他の機能を実行可能とする他機能実行手段を更に備えることを特徴とする請求項１０記載の日時管理機能内蔵署名作成装置。

【請求項１２】　前記日時管理機能内蔵署名作成装置において、

前記日時設定要求受付手段が最も最近受け付けた日時設定要求を行った日時管理者を日時設定者として、その情報を記憶する日時設定者情報記憶手段を更に備え、

前記署名作成手段が、前記日時の情報に加えて、日時設定者の情報を用いて署名を作成することを特徴とする請求項８、または９記載の日時管理機能内蔵署名作成装置。

【請求項１３】　前記日時管理機能内蔵署名作成装置において、

前記日時設定要求受付手段が現在までに受け付けた日時設定要求の数を記憶する日時設定回数情報記憶手段を更に備えると共に、

前記署名作成手段が、前記日時の情報に加えて、該日時設定回数情報を用いて署名を作成することを特徴とする請求項８、または９記載の日時管理機能内蔵署名作成装置。

【請求項１４】　入力データの暗号化または入力データに対する署名作成の機能を有するデータ処理装置において、

該データ処理装置の利用者が属する組織の管理者によって設定されるパスワードリトライ制限回数に対応して、利用者によるパスワードリトライ回数を制限す

るリトライ回数制限手段を備えることを特徴とするデータ処理装置。

【請求項１５】　入力データの暗号化または入力データに対する署名作成の機能を有するデータ処理装置において、

該データ処理装置の利用者が属する組織の管理者によって設定される最低パスワード長に対応して、利用者から与えられたパスワード更新要求内で更新後のパスワード長が該最低パスワード長以上である時に該パスワードの更新を行うパスワード更新手段を備えることを特徴とするデータ処理装置。

【請求項１６】　入力データに付けられた署名を検証する署名検証装置において、

該署名の検証の結果、該署名が入力データに対する正当な署名であるか否かを表示する署名検証結果表示手段を備えることを特徴とする署名検証装置。

【請求項１７】　複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理する方法において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、

該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後では該定められた日時管理者からの日時設定要求だけを受け付け、

該受け付けられた日時設定要求に対応して時計を動作させることを特徴とする日時管理方法。

【請求項１８】　階層構造をもつ複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理する方法において、

前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けた後には、該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付け、

該受け付けられた日時設定要求に対応して時計を動作させることを特徴とする日時管理方法。

【請求項１９】　複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理する計算機によって

使用される記憶媒体において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付けるステップと、

該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には、該あらかじめ定められた日時管理者からの日時設定要求だけを受け付けるステップと、

受け付けた日時設定要求に対応して時計を動作させるステップとを計算機に実行させるためのプログラムを格納した計算機読み出し可能可搬型記憶媒体。

【請求項２０】　階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理するための計算機によって使用される記憶媒体において、

前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けるステップと、

該任意の日時管理者からの日時設定要求を受け付けた後には該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付けるステップと、

該受け付けた日時設定要求に対応して時計を動作させるステップとを計算機に実行させるプログラムを格納した計算機読み出し可能可搬型記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば企業内、あるいは公的に有効な日時を管理する日時管理装置、およびそのように管理された時刻を用いて時刻付き署名を実現するための署名作成装置に関する。

【０００２】

【従来の技術と発明が解決しようとする課題】

日時管理装置は、例えば製造業などにおいて製品の製造時刻などを管理するために重要な装置であり、またそのように管理された時刻を用いて、時刻付き署名

を実現するための署名装置において重要である。例えば電子化したデータとしての領収書に対して、公的に認められる日時を記入することによって、その領収書の金額の改ざんなどを防止することが可能となる。

【０００３】

このような日時管理装置に対する日時設定方式としては、第１に特定の日時管理者からのみに日時設定を受け付ける、第２に不特定の任意の日時管理者からの日時設定も受け付ける、第３にユーザが日時管理者を指定できる、第４に日時管理装置が出荷される時に設定された日時の変更はできないというようないくつかの方法が存在した。

【０００４】

例えば時刻付き署名装置の場合には、不特定の日時管理者から日時設定を受け付けるようにすると署名日時の有効性が問題となり、またユーザが勝手に日時管理者を指定できても署名日時の有効性がなくなってしまう。このため一般に特定の日時管理者のみからの日時設定を受け付けるように設計されている。

【０００５】

しかしながら、実際の運用を考えると、公的に有効な時刻付き署名が求められる場合もあれば、例えば企業のようにある組織内だけで有効な時刻付き署名が求められる場合もあり、そのように署名の有効範囲を運用者側である程度自由に設定できることが望ましいが、従来の日時管理装置や時刻付き署名装置の場合には、そのように管理される日時の有効な範囲を弾力的に運用することはできないという問題点があった。

【０００６】

本発明の課題は、上述の問題点に鑑み、例えば企業あるいはそれに準ずる組織の日時管理者によって日時設定を行うことも可能であるが、組織の外部に対しても、有効な日時を管理するために特定の日時管理者、例えば国の日時管理センタからの日時設定を受け付けることによって、組織の外部に対しても有効な日時管理を行うことができる日時管理装置、およびそのような日時を用いた時刻付き署名装置を提供することである。

【０００７】

【課題を解決するための手段】

図１は本発明の原理構成ブロック図である。同図（ａ）は本発明の日時管理装置の原理構成ブロック図であり、日時管理装置１は、日時設定要求受付手段２と時計手段３とを備える。

【０００８】

本発明の日時管理装置１は複数の日時管理者からそれぞれ日時設定要求が入力されることのできるものであり、日時設定要求受付手段２は複数の日時管理者のうちで、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には、その定められた日時管理者からの日時設定要求だけを受け付けるものであり、時計手段３は受け付けた日時設定要求に対応して動作するものである。

【０００９】

また本発明の日時管理装置としては、階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理装置があり、この管理装置において日時設定要求受付手段２は、複数の日時管理者のうちで、任意の日時管理者からの日時設定要求を受け付けた後にはその任意の日時管理者よりも階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付けるものであり、時計手段３は受け付けた日時設定要求に対応して動作するものである。

【００１０】

発明の実施の形態においては、日時管理者側にも管理者用の日時管理装置を備え、その装置が管理する日時の複写の要求を前述の日時設定要求として、日時設定要求受付手段２に与える日時設定要求手段を備えることも、またその日時設定要求手段が日時設定要求を受け入れた日時管理装置から送られる非再現性の情報と、管理者用日時管理装置が管理する日時とを用いて、日時の複写のためのデータを生成する日時複写データ生成手段を更に備えることもできる。

【００１１】

更にこの日時複写データ生成手段は、非再現性の情報と前述の管理する日時の

情報とを暗号化して日時複写のためのデータを生成することも、またその暗号化した結果から署名を作成し、非再現性の情報、管理する日時、および署名を合わせて日時複写のためのデータを生成することもできる。

【００１２】

更に発明の実施の形態においては、日時管理装置の出荷元に更に日時管理装置を備え、その日時管理装置に日時を設定する日時設定手段を備えることもできる。

【００１３】

図１（ｂ）は本発明の日時管理機能内蔵署名作成装置の原理構成ブロック図である。この装置５は複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理機能を内蔵するものであり、日時設定要求受付手段６、時計手段７、および署名作成手段８を備える。

【００１４】

この日時管理機能内蔵署名作成装置５の内部の日時設定要求受付手段６は、図１（ａ）における日時設定要求受付手段２と同様の機能を持つものであり、また時計手段７も時計手段３と同様の機能を持つ。署名作成手段８は、時計手段７が示す日時の情報を用いて、入力される署名対象データに対する署名を作成するものである。

【００１５】

本発明の日時管理機能内蔵署名作成装置としては、階層構造をもつ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理機能を内蔵する装置も可能であり、この装置において日時設定要求受付手段は複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け入れた後には、その任意の日時管理者よりも階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付けるものであり、時計手段７は受け付けた日時設定要求に対応して動作するものであり、署名作成手段８は時計手段７が示す日時の情報を用いて、入力される署名対象データに対する署名を作成するものである。

【００１６】

発明の実施の形態においては、日時管理機能内蔵署名作成装置５は、時計手段

７の動作停止が検出された時、署名作成手段８による署名作成を停止させる署名停止手段を更に備えることも、また署名作成装置５が署名作成の機能と異なる１つ以上のほかの機能をさらに備え、時計手段７の動作停止が検出された時、署名作成の機能と異なるほかの機能を実行可能とする他機能実行手段を更に備えることもできる。

【００１７】

発明の実施の形態においては、日時設定要求受付手段６が最も最近受け付けた日時設定要求を行った日時管理者を日時設定者として、その情報を記憶する日時設定者情報記憶手段を更に備え、署名作成手段８が日時の情報に加えて日時設定者の情報を用いて署名を作成することもでき、あるいは日時設定要求受付手段が現在までに受け付けた日時設定要求の数を記憶する日時設定回数情報記憶手段を更に備え、署名作成手段８が日時の情報に加えて日時設定回数情報を用いて署名を作成することもできる。

【００１８】

本発明の入力データの暗号化または入力データに対する署名作成の機能を有するデータ処理装置は、そのデータ処理装置の利用者が属する組織の管理者によって設定されるパスワードリトライ制限回数に対応して、利用者によるリトライ回数を制限するリトライ回数制限を備えている。

【００１９】

また本発明において入力データの暗号化または入力データに対する署名作成の機能を有するデータ処理装置は、そのデータ処理装置の利用者が属する組織の管理者によって設定される最低パスワード長に対応して、利用者から与えられたパスワード更新要求内で更新後のパスワード長がその最低パスワード長以上である時に、パスワード更新を行うパスワード更新手段を備える。

【００２０】

本発明において入力データに付けられた署名を検証する署名検証装置は、署名の検証の結果、その署名が入力データに対する正当な署名であるか否かを表示する署名検証結果表示手段を備える。

【００２１】

本発明の日時管理方法として、複数の日時管理者からそれぞれ日時設定要求が入力されることのできる場合において、複数の日時管理者のうちで、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後にはその定められた日時管理者からの日時設定要求だけを受け付け、受け付けた日時設定要求に対応して時計を動作させる方法が用いられる。

【００２２】

本発明における署名作成方法として、複数の日時管理者からそれぞれ日時設定要求が入力されることができる日時管理機能を内蔵する署名作成装置において、複数の日時管理者のうちであらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後にはその定められた日時管理者からの日時設定要求だけを受け付け、受け付けた日時設定要求に対応して時計を動作させ、時計が示す日時の情報を用いて入力される署名対象データに対する署名を作成する方法が用いられている。

【００２３】

本発明において複数の日時管理者からそれぞれ日時設定要求が入力されることができ、日時を管理する計算機によって使用される記憶媒体において、複数の日時管理者のうちであらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付けるステップと、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には定められた日時管理者からの日時設定要求だけを受け付けるステップと、受け付けた日時設定要求に対応して時計を動作させるステップとを備えるプログラムを格納した計算機読み出し可能可搬型記憶媒体が用いられる。

【００２４】

更に本発明における記憶媒体として、複数の日時管理者からそれぞれ日時設定要求が入力されることができる日時管理機能を内蔵し、署名を作成するための計算機によって使用される記憶媒体において、複数の日時管理者のうちで、あらか

じめ定められた日時管理者からの日時設定要求を受け付ける前には、任意の日時管理者からの日時設定要求を受け付けるステップと、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には定められた日時管理者からの日時設定要求だけを受け付けるステップと、受け付けた日時設定要求に対応して時計を動作させるステップと、時計が示す日時の情報を用いて入力される署名データに対する署名を作成するステップとを計算機に実行させるプログラムを格納した計算機読み出し可能可搬型記憶媒体が用いられる。

【００２５】

以上のように本発明によれば、複数の日時管理者のうちで特定の日時管理者からの日時設定要求が優先されるか、または階層構造を持つ複数の日時管理者のうちで上位の日時管理者からの日時設定要求が優先して受け付けられる。

【００２６】

【発明の実施の形態】

本発明の実施の形態としては、日時管理装置と、日時管理機能を内蔵した時刻付き署名装置の２つを中心として説明する。例えば時刻付き署名装置は、ユーザが電子化された文書に対して、日付や印鑑のかわりに時刻付き署名を付けるものである。この時刻付き署名の有効性は、当然管理されている日時の有効性によって支配される。

【００２７】

狭い範囲としては、例えば企業内でその日時が有効であれば足りることもあり、例えば公証役場で作成される書類のように公的なものとして有効にしたい場合には、管理されている日時が例えば国によって保証されている必要があり、国の日時管理センタのような機関によって管理されている日時と同一の日時を管理する必要がある。

【００２８】

次に日時管理者とユーザとの関係については、特に規定を行うことは必要がない。具体的な例として企業内のユーザを考える場合には、日時管理者は企業内のシステム管理者であり、後述する特定の日時管理者は国の日時管理センタであったり、装置の出荷元である場合などが考えられる。

【００２９】

装置の出荷元では、ユーザの運用形式として企業内でのみ有効な時刻付き署名を行うのか、公的にも有効な時刻付き署名を行うのかに対応させて装置を別々に出荷することは大変であり、また公的な時刻付き署名の機能を企業内だけの時刻付き署名だけを用いるユーザにも押し付けることにも問題があり、更に運用途中で時刻付き署名の有効範囲の拡大を行いたい場合も考えられる。

【００３０】

このため装置の出荷元からの出荷時においては、例えば企業内の日時管理者からの時刻設定を行えるようにしておき、一旦特定の管理者、例えば国の日時管理センタからの日時設定を受け付けると、以後はその特定の管理者からだけの設定を受け付けるようにする必要がある。

【００３１】

図２は本発明の日時管理装置における基本的な日時設定方式の説明図である。同図においてユーザ側日時管理装置１０に対して、最初は任意の日時管理者からの日時設定を受け付けることができるものとする。例えばユーザが属する企業の日時管理者の日時管理装置１１から、まず（１）において日時情報がユーザ側日時管理装置１０の内部の時計１３に設定される。この時企業内の日時管理者は、特定の日時管理者、例えば国の日時管理センタの日時管理者や、装置の製造元の日時管理者などではないため、日時情報が時計１３に設定されても、フラグ１４はオフのままとなっているものとする。

【００３２】

このフラグ１４は、ユーザ側日時管理装置１０内の時計１３に日時情報が設定される際には必ずチェックされる。そしてフラグがオフの場合に、特定の日時管理者、例えば前述の国の日時管理センタ側からの日時設定を受け付けた時点でフラグがオンとされる。

【００３３】

図２において国の日時管理センタ、すなわち特定の日時管理者の日時管理装置１２によって、（２）において日時情報がユーザ側日時管理装置１０に対して設定されると、その日時情報に従って時計１３の動作が行われるようになると共に

、フラグ１４がオンとされる。

【００３４】

このようにフラグ１４がオンとなった後には、ユーザ側日時管理装置１０は特定の日時管理者側からの日時設定は受け付けるものの、それ以外の日時管理者からの日時情報の設定は受け付けない。すなわち（３）において、特定の日時管理者の日時管理装置１２から日時情報を設定すること、すなわち日時情報を変更することは可能であるが、例えば企業側の日時管理者の日時管理装置１１から（４）において日時情報を設定しようとしても、ユーザ側日時管理装置１０はその設定を受け付けない。

【００３５】

図３は日時管理装置の階層構造の説明図である。同図において，日時管理装置２１～２５は最下位の日時管理装置であり、そのうち日時管理装置２１～２３は領域Ａに、また５つの日時管理装置２１～２５は領域Ｂに属するものとする。

【００３６】

日時管理装置２６、２７は中間階層の日時管理装置であり、装置２６は領域Ａの日時管理装置２１～２３の上位に属し、また装置２７は領域Ｂのうちで領域Ａを除いた部分、すなわち日時管理装置２４、２５の上位の管理装置である。

【００３７】

日時管理装置２８は最上位階層の装置であり、中間階層の日時管理装置２６および２７の上位に属している。

日時管理装置が管理する日時情報は、当然ある領域においてはその有効性が保証されなければならない。例えば日時管理装置２１に対して日時管理装置２６から日時設定が行われた場合には、日時管理装置２１は領域Ａ内で日時が保証される日時管理装置として動作することになり、日時管理装置２６を介して最上位の日時管理装置２８から日時設定を受けた場合には、日時管理装置２１は領域Ｂにおいて日時情報が保証される日時管理装置として動作することになる。

【００３８】

このように一旦最上位階層の日時管理装置２８からの日時設定を受けて、領域Ｂ内で日時情報が保証される装置として動作するようになった場合に、中間階層

の日時管理装置２６から日時の再設定、すなわち変更を受け付けると領域Ａ内でしか保証されない日時情報が設定されてしまうために、日時管理装置２６からの日時設定は受け付けない。例えば中間階層の日時管理装置２７の下位にある日時管理装置２４についても同様である。図３では日時管理装置が３層の階層構造のもつものとしたが、４層以上の階層においても同様の動作が行われる。

【００３９】

日時管理者、あるいは日時設定機関の階層構造としては、例えば最上位に世界的な機関、中間に各国毎の機関、最下位に企業毎の機関を備える階層構造を考えることもでき、あるいは最上位に日本の機関、中間に装置の出荷元の機関、最下位に企業毎の機関を備えるようにすることもでき、また更に階層を増やすことも可能である。

【００４０】

また図３において最下位の日時管理装置、一般にユーザの日時管理装置と、中間の日時管理装置、および最上位の日時管理装置との間で、基本的な動作は同じである。ただ最上位の日時管理装置は日時の設定動作だけ行うものであり、最下位のユーザの日時管理装置は日時の設定を受けるだけと考えれば、動作はその部分では異なる。

【００４１】

またユーザの日時管理装置は、ユーザの勝手な日時変更から設定された時刻を守るために、筐体などで守られている必要があるが、中間あるいは最上位の日時管理装置は、例えば厳重に管理されたサーバルームに置かれているサーバの形式でもよく、装置の形態は大きく異なる可能性がある。

【００４２】

後述する時刻付き署名装置の場合にも、上位の装置に署名機能が必要か否かによって、上位の装置と下位の装置との機能が同一か否かが決定される。上位の装置が日時設定だけを行う場合には、署名機能は必要はないが、上位の装置でも下位の装置の署名を検証したり、上位の装置として署名機能を持つ場合には、上位側の装置も下位側の装置と同じ動作を行う署名装置となる。

【００４３】

図４は本発明の時刻付き署名装置に対する日時情報の基本的な設定方式の説明図である。同図においてユーザ側時刻付き署名装置３０の内部には、図２におけると同様に時計１３とフラグ１４が備えられており、図２におけると同様にフラグ１４がオフの状態では、例えばユーザの属する企業の日時管理者の日時管理装置１１からも、また例えば国の時刻管理センタの日時管理装置１２からも時刻の設定が可能である。

【００４４】

しかしながら図２におけると同様に、一旦特定の日時管理者の日時管理装置１２からの日時設定を受け付け、その情報が時計１３に設定されると、この特定の日時管理者側からの日時情報の設定以外は受け付けられなくなる。

【００４５】

ユーザ側時刻付き署名装置３０に外部から署名対象データ３１が入力されると、そのデータと時計１３から出力される日時情報とが３２で連結され（例えばデータビットの後に日時情報のビットが並べられ）、署名鍵３３を用いて、３４で署名が作成され、外部に対して日時情報と署名３５が出力される。

【００４６】

図５は時刻付き署名装置に対する日時管理の階層構造の説明図である。同図においては、図３の日時管理装置２１～２５に代わって、最下位の階層に時刻付き署名装置４１～４５が位置している。

【００４７】

各時刻付き署名装置に対する日時設定方式は図３におけると全く同様であり、例えば時刻付き署名装置４１は日時管理装置２６を介して最上位の日時管理装置２８からの日時設定を受け付けると、それ以後は中間階層の日時管理装置２６からの日時設定が受け付けない。日時管理装置２７の下位にある時刻付き署名装置４４に対する日時設定についても全く同様である。

【００４８】

続いて本実施例形態における日時管理装置の動作について、図６～図１０を用いて更に説明する。図６は日時管理装置に対する日時設定の処理フローチャートであり、図２に対応する処理のフローチャートである。同図において日時設定要

求、例えば図２における企業内の日時管理者の日時管理装置１１からの日時設定要求に対応して処理が開始され、まずステップＳ１でフラグ１４の値がチェックされ、ステップＳ２でフラグの値がオンかオフかが判定される。

【００４９】

図２において例えば国の日時管理センタの日時管理装置１２側からの日時設定がまだ行われていない場合にはフラグはオフであり、その時にはステップＳ３で日時設定要求を行っているのが特定の日時管理者であるか否かが判定される。例えば国の日時管理センタ側のような特定の日時管理者でない場合には、ステップＳ４で日時が時計１３に設定されて処理を終了する。特定の日時管理者である場合は、ステップＳ５で日時設定が行われると共にフラグ１４がオンとされて処理を終了する。

【００５０】

なお、ここでは最初はフラグがオフとなっていて特定の日時管理者以外でも日時設定を行えるものとしたが、例えば出荷時にフラグがオンとされることによって、特定の日時管理者のみが日時を設定できるようにすることも可能である。

【００５１】

ステップＳ２でのフラグの値がオンである時、すなわちすでに特定の日時管理者側からの日時設定が行われている場合には、ステップＳ６で日時設定要求を行っているのがその特定の日時管理者であるか否かが判定され、特定の日時管理者である場合にはステップＳ７で日時の設定が行われた後に、特定の日時管理者でない場合には直ちに処理を終了する。特定の日時管理者でない場合には必要に応じてエラー通知などが行われるが、その説明は省略する。

【００５２】

なお本実施形態においては、特定の日時管理者から日時設定が行われたか否かをフラグの値によって管理しているが、この管理には必ずしもフラグを用いる必要はなく、特定の日時管理者からの日時設定が行われたか否かを認識することができれば、どのような手段を用いて管理を行っても差し支えないことは当然である。

【００５３】

図７は日時設定処理のフローチャートであり、図３のように日時管理装置が階層構造を持つ場合の処理フローチャートである。

図７において日時設定要求に対応して処理が開始されると、まずステップＳ１０で日時設定要求者がチェックされ、ステップＳ１１で日時設定要求者が上位階層の日時管理者か、日時設定者か、あるいは下位階層、または同階層ではあるが日時設定者でない日時管理者であるかが判定される。ここで日時設定者とは、図２の日時管理装置１０の時計１３にその時点で有効となっている日時情報を設定して日時管理者、すなわち最も最新の日時情報設定者であり、後述するようにこの情報は日時管理装置の内部のメモリに記憶されているものとする。

【００５４】

日時設定者、すなわち最も新しく日時を設定した日時管理者である場合には、ステップＳ１２で日時設定、すなわち日時の変更が行われ処理を終了する。

日時設定要求者が上位階層の日時管理者である場合には、ステップＳ１３で日時設定が行われ、必要に応じて、すなわちその上位階層の日時管理者が現在装置内に記憶されている日時設定者と異なる場合には日時設定者の変更も行われて、処理を終了する。

【００５５】

ステップＳ１１で日時設定要求者が下位階層の日時管理者、または同一階層であっても装置に記憶されている日時設定者でない日時管理者である場合には、日時が設定されることなく、処理を終了する。

【００５６】

図８は本実施形態における日時管理装置の運用例の説明図である。同図においてユーザ側、例えば企業内には一般ユーザ向けの日時管理装置、一般に複数の日時管理装置５０と、ユーザ側管理者用の日時管理装置５１が存在し、ユーザ用の日時管理装置５０はユーザ側管理者の日時管理装置５１によって管理されるものとする。例えば日時管理装置が出荷される状態では、管理者の日時管理装置５１だけに対して、上位側の日時管理者の日時管理装置５２によって日時設定が行われる。この上位側の日時管理装置は、例えば国の日時管理センタの装置でも、また出荷元に備えられている装置でもよい。

【００５７】

日時管理装置の出荷後に、ユーザの日時管理装置５０の初期化がユーザ側管理者によって行われる。この初期化と同時に、ユーザ側管理者の日時管理装置５１の日時が複数のユーザの日時管理装置５０に複写され、これによってユーザ側の組織、例えば企業内ではユーザ側管理者の日時管理装置５１の日時と同期して全ての日時管理装置の運用が可能となる。

【００５８】

なおユーザ側管理者の日時管理装置５１に対する日時設定や、ユーザの日時管理装置５０への日時設定は、出荷時または初期化時に限定されるものではなく、適当な時期に行ってもよいことは当然である。また出荷時にはユーザ側管理者の日時管理装置５１だけに日時が設定されるものとしたが、ユーザの日時管理装置５０に対する日時設定を出荷時に行ってもかまわないことも当然である。

【００５９】

図９は図８における日時情報複写方式の詳細説明図である。同図においてユーザの日時管理装置５０と、ユーザ側管理者の日時管理装置５１の内部には、共通の秘密鍵Ｋｔ５５が格納されているものとする。

【００６０】

例えば管理者の日時管理装置５１からの日時設定要求に対応して、ユーザの日時管理装置５０は（１）で乱数を生成し、これを管理者の日時管理装置５１側に送る。この乱数は非再現性の情報であればよく、例えば連番などであってもよい。

【００６１】

ここで例えば乱数をユーザ側から送るのは管理者側からの日時情報の再送を防止するためである。乱数を送った直後に送られるに日時情報をユーザ側は必要としており、例えば１週間前の日時情報の再送は不適当である。

【００６２】

管理者の日時管理装置５１では、（２）において送られた乱数と日時情報を連結し、秘密鍵Ｋｔ５５を用いて（３）で連結された情報を暗号化して、ユーザの日時管理装置５０に送る。

【００６３】

このように乱数と日時情報とを連結して暗号化して送る代わりに、鍵Ｋｔを用いた署名を作成し、その署名と、乱数および日時情報を連結したデータそのまま、すなわち平文とを送ってもよい。署名の方式については後述する。また鍵Ｋｔ５５としては、複数のユーザ側日時管理装置５０に共通の鍵であってもよく、装置毎に異なる鍵でもよい。更にこのような秘密鍵の代わりに公開鍵を用いて暗号化したり、プライベート鍵を用いて署名を作成してもよい。

【００６４】

後述するＤＥＳ－ＭＡＣ方式の署名の場合には、最終的な出力８バイトのうちの上位の４バイトだけが署名として用いられる。これに対して、前述の乱数と日時情報を連結して暗号化する場合には、最終的な暗号化出力の全てが暗号化の結果として用いられ、ユーザ側に送られることになる。そして暗号化の代わりに署名が用いられる場合には、ユーザ側で後述するような署名のチェックを行うことによって、日時管理者側から送られてくる日時設定メッセージの正当性を確認することができる。

【００６５】

ユーザの日時管理装置５０においては、受け取った情報を（４）で秘密鍵Ｋｔを用いて復号し、その結果得られた乱数を（５）で（１）において生成した乱数と比較し、生成した乱数と一致した場合には日時情報を（６）で時計に設定して日時の複写を終了する。

【００６６】

図１０はユーザの日時管理装置への日時情報の複写方式の他の例の説明図である。同図においては、図９における日時情報の複写に加えて、図７で説明した日時設定者の情報と、日時の設定回数の情報をメモリに格納する日時設定方式の説明図である。

【００６７】

図１０において、まず（１）でユーザの日時管理装置５０の内部で乱数が生成され、例えばユーザ側管理者の日時管理装置５１に送られる。ユーザ側管理者の日時管理装置５１では、送られた乱数と日時情報６４とが（２）で連結され、鍵

Ｋｔ６５を用いて（３）で連結された情報が暗号化され、更に（４）で設定者情報６６が、暗号化された情報と連結されて、ユーザの日時管理装置５０に送られる。

【００６８】

ユーザの日時管理装置５０では、送られた情報から設定者情報６６を取り出し、現在日時を設定しようとしている日時管理者、ここではユーザ側管理者に対応する鍵Ｋｔ６５を用いて（６）で受け取った情報を復号し、復号した情報の中の乱数を取り出して、（１）で自装置で生成し、ユーザ管理者側に送った乱数と（７）で比較する。

【００６９】

２つの乱数の比較の結果、両者が一致すれば、受け取った日時情報に対応して時計６７の動作が制御されるとともに、設定者情報６６がメモリ６８に格納され、また日時設定回数情報６９がインクリメントされる。ここでメモリ６８に以前の日時設定者の情報が格納されている場合には、その情報は必要に応じて更新される。設定者情報の内容は設定者ＩＤや、前述の階層などである。

【００７０】

ユーザの日時管理装置５０の側で受け取ったデータのうち設定者情報６６を取り出すのは、データの復号に使う鍵として複数の日時管理者にそれぞれ対応する鍵が格納されており、現在日時を設定しようとしている管理者、ここではユーザ側管理者に対応する鍵を用いて復号を行うためである。

【００７１】

また日時設定回数情報をインクリメントするのは、日時管理装置が管理する日時情報の整合性を保つためである。例えばユーザの日時管理装置５０の時計６７が１時間進んでおり、ユーザ側管理者の日時管理装置５１から時間を１時間戻すための日時情報の設定が行われたとする。この場合、例えばユーザの日時管理装置５０の管理下で製造される製品の製品番号と製造時刻との対応がずれてしまうことになる。ここで日時設定回数をカウントすることによって、製造時刻が前でも、実際の製造は後に行われたということが認識可能となる。

【００７２】

図１１は日時管理装置内の時計の精度の維持方式の説明図である。同図において、例えばユーザの日時管理装置５０の内部には日時設定処理回路５６があり、例えば図９でユーザ側管理者の日時管理装置５１から送られた日時設定情報がこの処理回路５６によって処理され、前述のように乱数の比較の結果が正しい場合には、受け取った日時情報がリアルタイムクロック（ＲＴＣ）５７の内部の日時情報５８に設定される。

【００７３】

このリアルタイムクロック５７では、水晶振動子の固体特性による発振周波数のバラつきを補正し、時計の精度を上げるために発振器の分周比を変える補正情報５９が用いられる。このようなリアルタイムクロック５７ではバッテリーのバックアップが切れると、設定されている補正情報５９の値が消えてしまうため、本実施形態においてはこの補正情報を不揮発性メモリ６０に格納し、例えばバッテリーのバックアップが切れた場合に外部からの日時設定に続いて、不揮発性メモリ６０に格納されている補正情報６１を読み込み、リアルタイムクロック５７に設定することによって時計の精度の保証が行われる。

【００７４】

なお本実施形態ではリアルタイムクロック５７の電源として２次電池を用いるものとする。２次電池を用いることにより、電源が復旧すれば電池が充電され、時計の再駆動が行われる。

【００７５】

続いて時刻付き署名装置の実施形態について図１２～図１９を用いて説明する。図１２は時刻付き署名作成要求、すなわち図４で説明したように署名対象データ３１が外部から与えられ、時刻付き署名の作成が要求された場合の全体処理フローチャートである。

【００７６】

図１２において処理が開始されると、まずステップＳ２０で時計がきちんと動いていて日時情報が信用できるかがチェックされ、ステップＳ２１で時計が停止しているか（あるいは一時停止していたか）否かが判定され、停止していない場合にはステップＳ２２で署名が生成されて処理を終了し、また時計が停止してい

る場合にはステップＳ２３でエラー通知が行われて、処理を終了する。

【００７７】

図１３は時刻付き署名装置の全体処理フローチャートの他の例である。同図においては、時刻付き署名装置は図４で説明したような署名作成処理だけに限定されることなく、例えば後述するように署名検証処理や、入力データの単なる暗号化処理などのように、時刻を利用しない処理も実行できるものとする。

【００７８】

図１３において外部からの処理要求に対して処理が開始されると、まずステップＳ２５で要求解析が行われ、ステップＳ２６でその処理要求が正確な時刻を利用する処理の要求であるか否かが判定され、時刻を利用する要求である時には図１２におけると同様にステップＳ２１～Ｓ２３の処理が行われる。これに対して時刻を利用しない処理の要求である場合には、ステップＳ２７で要求された処理が実行され、処理を終了する。

【００７９】

図１４は時刻付き署名装置における署名作成方式の詳細説明図である。同図においては時刻付き署名装置７０の内部で、図４の時計以外に、図１０で説明した日時設定回数情報７２、設定者情報７３、および装置の識別子としての装置ＩＤ７４がメモリに格納されている。

【００８０】

日時設定回数情報７２としては設定回数が、例えば８バイトのバナリーデータとして格納され、設定者情報７３としてはこれも例えば８バイトのデータとして、設定者の名前やＩＤを表すデータや、システム的に設定者が２人に限定されている場合にはフラグのように１／０の値を持つデータが格納される。また装置ＩＤ７４としても、８バイトのデータが格納されているものとする。

【００８１】

図１４において署名対象データが外部から入力されると、時計７１の出力としての日時情報（年、月、日、時、分、秒）、日時設定回数情報７２、設定者情報７３、および装置ＩＤ７４が署名対象データと７５で連結され、署名鍵７６を用いて７７で署名が作成されて、外部に対して設定者情報、装置ＩＤ、日時設定回

数情報、日時情報、および署名が出力される。ここで署名以外の出力は例えば全て暗号化されていないデータ、すなわち平文として出力される。

【００８２】

図１５は本実施形態における署名作成方式の説明図である。本実施形態においては、ＤＥＳ－ＭＡＣの署名方式を用いることとする。モードとしてはＣＢＣモードを使用して署名作成が行われる。まず署名対象データが８バイトずつのブロックに分割され、署名対象データ１～署名対象データＮが得られる。

【００８３】

図１５においてまず署名対象データ１、８バイトに対して８０で初期値ＩＶ８１を０として排他的論理和の演算が行われ、その出力に対して演算処理Ｅ８２で署名鍵を用いて暗号化が行われる。その暗号化結果は次の署名対象データ２に対する排他的論理和８０への一方の入力として与えられる。

【００８４】

同様の動作が行われ、署名対象データＮに対する排他的論理和８０と、署名鍵を用いた暗号化が８２が行われ、その結果は、設定者情報７３、８バイトが入力される排他的論理和８０に対して入力され、署名鍵を用いた暗号化８２が行われる。

【００８５】

同様に日時設定回数情報７２、日時情報、および装置ＩＤ７４に対して演算が行われ、最終的出力として８バイトが得られる。この８バイト出力のうち上位４バイト、すなわち３２ビットがＤＥＳ－ＭＡＣの署名結果とされる。

【００８６】

図１６は前述のように時刻付き署名装置が署名作成だけでなく、署名検証機能を有する場合の署名検証方式の説明図である。同図において時刻付署名検証装置８３に対して外部から署名検証のために署名対象データ、装置ＩＤ、設定者情報、日時設定回数情報、日時情報と共に署名が入力される。

【００８７】

時刻付き署名検証装置８３においては、入力されたデータ（署名を除く）と署名鍵８４を用いて、８５で署名が再生され、再生された署名と入力されたデータ

のうちの署名とが８６で比較され、両者が一致すれば署名は正しいことが検証され、例えば緑のＬＥＤ８７が点灯することによって署名が正しかったことが表示される。

【００８８】

比較８６の結果、正しくないと判定された場合には赤のＬＥＤ８８が点灯することによって、署名が正しくないことが表示される。これらのＬＥＤの表示は、例えば一定時間後に自動的に消えるか、あるいは外部からの入力によって消えるようにすることが可能である。

【００８９】

図１７は時刻付き署名装置に対するパスワードリトライ回数と最低パスワード長の設定方式の説明図である。時刻付き署名装置の出荷時には、パスワードリトライ回数や最低パスワード長としては、システムとして固定の値を設定することができる。固定の値としては、リトライ回数には制限がなくてもよく、また最低パスワード長は１文字でもかまわない。

【００９０】

図８で説明した場合と同様に、ユーザ側管理者が一般ユーザ向けの時刻付き署名装置の初期化を行うにあたってユーザ登録と共に、パスワードリトライ回数と最低パスワード長の設定を行うものとする。

【００９１】

図１７において、例えばユーザ側管理者によりユーザ情報、最低パスワード長、リトライ回数制限情報に署名が付加されて、時刻付き署名装置７０に与えられる。

【００９２】

時刻付き署名装置７０では、ユーザ側管理者と共通の装置鍵９０を用いて、９１で署名の検証を行い、署名結果が正しい場合にはメモリにユーザ情報９２、最低パスワード長９３、およびリトライ回数制限情報９４を格納する。ここでユーザ情報は、ユーザＩＤのように利用者認証に用いるデータや、署名鍵などである。

【００９３】

図１８は本実施形態におけるパスワード更新処理のフローチャートである。同図においてパスワード更新命令に対応して処理が開始されると、ステップＳ３０でパスワードの長さが検出され、ステップＳ３１でその長さが最低パスワード長と比較され、最低パスワード長以上であればステップＳ３２でパスワードが更新された後に、最低パスワード長より短い場合にはステップＳ３３でエラー通知が行われて、処理を終了する。

【００９４】

図１９は本実施例におけるパスワードリトライ回数制限処理のフローチャートである。同図においてパスワードが入力され、処理が開始されると、まずステップＳ３５で入力されたパスワードと装置に登録されているパスワードが一致しているか否かが判定され、一致している場合には、ステップＳ３６でリトライ回数がクリアされて処理を終了する。リトライ回数がもともとクリアされている状態の場合には、ステップＳ３６の処理は必要ない。

【００９５】

ステップＳ３５でパスワードが一致しないと判定されると、ステップＳ３７で現在のパスワードリトライ回数、すなわち前回までのパスワードリトライ回数が回数制限情報と比較され、回数制限情報未満である時にはステップＳ３８でリトライ回数がインクリメントされて処理を終了し、前回までの、リトライ回数がすでに回数制限情報の回数に達している場合には、ステップＳ３９で動作が停止されて処理を終了する。ここでリトライ回数制限情報は、リトライ回数がその回数に達しても装置の動作は停止されず、その回数を超えた時に装置の動作が停止するリトライ回数を示すものとする。

【００９６】

最後に本実施形態におけるプログラムのコンピュータへのローディングについて説明する。本実施形態における日時管理装置、および時刻付き署名装置は、当然一般的なコンピュータによって実現することができる。

【００９７】

図２０はそのようなコンピュータの構成ブロック図である。同図においてコンピュータ９５は、本体９６とメモリ９７によって構成されている。メモリ９７と

しては、ランダムアクセスメモリ（ＲＡＭ）ハードディスク、磁気ディスクなどの様々な記憶装置を用いることが可能である。

【００９８】

本発明の特許請求の範囲第１９項、第２０項のプログラムや、図６，図７，図１２，図１３，図１８、および図１９のフローチャートに示されるプログラムなどがメモリ９７に格納され、そのプログラムが本体９６によって実行されることによって、本実施形態における日時管理装置、および時刻付き署名装置の動作を実現することが可能となる。

【００９９】

このようなプログラムは、プログラム提供者側からネットワーク９８を介してコンピュータ９５にロードされることによって、あるいは市販され、流通している可搬型記憶媒体９９に格納され、そのプログラムがコンピュータ９５にロードされることによって、実行されることも可能である。可搬型記憶媒体９９としてはフロッピーディスク、ＣＤ－ＲＯＭ、光ディスク、光磁気ディスクなど、様々な形式の記憶媒体を利用することができ、このような記憶媒体に前述のプログラムなどが格納され、このプログラムがコンピュータ９５によって実行されることによって、日時管理装置および時刻付き署名装置の動作を実現することができる。

【０１００】

（付記１）複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理装置において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には、該あらかじめ定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段とを備えることを特徴とする日時管理装置。（１）

該受け付けられた日時設定要求に対応して動作する時計手段とを備えることを

特徴とする日時管理装置。

【０１０１】

（付記２）階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理装置において、

前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けた後には、該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段とを備えることを特徴とする日時管理装置。

【０１０２】

（付記３）前記日時管理者側に管理者用の日時管理装置を備え、

該管理者用日時管理装置が、自装置が管理する日時の複写の要求を前記日時設定要求として前記日時設定要求受付手段に与える日時設定要求手段を備えることを特徴とする付記１、または２記載の日時管理装置。

【０１０３】

（付記４）前記日時設定要求手段が、前記日時設定要求を受け付けた日時管理装置から送られた非再現性の情報と、前記管理者用日時管理装置が管理する日時とを用いて、前記日時の複写のためのデータを生成する日時複写データ生成手段を更に備えることを特徴とする付記３記載の日時管理装置。

【０１０４】

（付記５）前記日時複写データ生成手段が、前記非再現性の情報と前記管理する日時の情報とを暗号化して、日時複写のためのデータを生成することを特徴とする付記４記載の日時管理装置。

【０１０５】

（付記６）前記日時複写データ生成手段が、前記非再現性の情報と前記管理する日時の情報とを暗号化した結果から署名を作成し、該非再現性の情報、管理する日時、および署名を合わせて日時複写のためのデータを生成することを特徴とする付記４記載の日時管理装置。

【０１０６】

（付記７）前記日時管理装置の出荷元に更に日時管理装置を備えると共に、

該出荷元の日時管理装置が、前記管理者用日時管理装置の出荷時に、該管理者用日時管理装置に日時を設定する日時設定手段を備えることを特徴とする付記３記載の日時管理装置。

【０１０７】

（付記８）前記日時管理装置において、

前記時計手段の精度を向上させるための補正情報を格納する不揮発性記憶手段を更に備えることを特徴とする付記１、または２記載の日時管理装置。

【０１０８】

（付記９）前記日時管理装置において、

前記時計手段の電源が切れ、電源が再投入された後に前記日時設定要求受付手段が日時設定要求を受け付けた時点で、前記不揮発性記憶手段に記憶されている補正情報を該時計手段に再設定する補正情報再設定手段を更に備えることを特徴とする付記８記載の日時管理装置。

【０１０９】

（付記１０）前記時計手段の電源として、二次電池を備えることを特徴とする付記８または、９記載の日時管理装置。

（付記１１）複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理機能を内蔵する署名作成装置において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には該あらかじめ定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段と、

該時計手段が示す日時の情報を用いて、入力される署名対象データに対する署名を作成する署名作成手段とを備えることを特徴とする日時管理機能内蔵署名作成装置。

【０１１０】

（付記１２）階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる日時管理機能を内蔵する署名作成装置において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には該あらかじめ定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けた日時設定要求に対応して動作する時計手段と、

該時計手段が示す日時の情報を用いて、入力される署名対象データに対する署名を作成する署名作成手段とを備えることを特徴とする日時管理機能内蔵署名作成装置。

【０１１１】

（付記１３）前記日時管理機能内蔵署名作成装置において、

前記時計手段の動作停止が検出された時、前記署名作成手段による署名作成を停止させる署名停止手段を更に備えることを特徴とする付記１１、または１２記載の日時管理機能内蔵署名作成装置。

【０１１２】

（付記１４）前記日時管理機能内蔵署名作成装置が、前記署名作成の機能と異なる1 つ以上の他の機能を更に備えると共に、

前記時計手段の動作停止が検出された時、該署名作成の機能と異なる他の機能を実行可能とする他機能実行手段を更に備えることを特徴とする付記１３記載の日時管理機能内蔵署名作成装置。

【０１１３】

（付記１５）前記日時管理機能内蔵署名作成装置において、

前記日時設定要求受付手段が最も最近受け付けた日時設定要求を行った日時管理者を日時設定者として、その情報を記憶する日時設定者情報記憶手段を更に備え、

前記署名作成手段が、前記日時の情報に加えて、日時設定者の情報を用いて署名を作成することを特徴とする付記１１、または１２記載の日時管理機能内蔵署

名作成装置。

【０１１４】

（付記１６）前記日時管理機能内蔵署名作成装置において、

前記日時設定要求受付手段が現在までに受け付けた日時設定要求の数を記憶する日時設定回数情報記憶手段を更に備えると共に、

前記署名作成手段が、前記日時の情報に加えて、該日時設定回数情報を用いて署名を作成することを特徴とする付記１１、または１２記載の日時管理機能内蔵署名作成装置。

【０１１５】

（付記１７）入力データの暗号化または入力データに対する署名作成の機能を有するデータ処理装置において、

該データ処理装置の利用者が属する組織の管理者によって設定されるパスワードリトライ制限回数に対応して、利用者によるパスワードリトライ回数を制限するリトライ回数制限手段を備えることを特徴とするデータ処理装置。

【０１１６】

（付記１８）入力データの暗号化または入力データに対する署名作成の機能を有するデータ処理装置において、

該データ処理装置の利用者が属する組織の管理者によって設定される最低パスワード長に対応して、利用者から与えられたパスワード更新要求内で更新後のパスワード長が該最低パスワード長以上である時に該パスワードの更新を行うパスワード更新手段を備えることを特徴とするデータ処理装置。

【０１１７】

（付記１９）入力データに付けられた署名を検証する署名検証装置において、

該署名の検証の結果、該署名が入力データに対する正当な署名であるか否かを表示する署名検証結果表示手段を備えることを特徴とする署名検証装置。

【０１１８】

（付記２０）複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理する方法において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付け、

該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後では該定められた日時管理者からの日時設定要求だけを受け付け、

該受け付けられた日時設定要求に対応して時計を動作させることを特徴する日時管理方法。

【０１１９】

（付記２１）階層構造をもつ複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理すること方法において、

前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けた後には、該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付け、

該受け付けられた日時設定要求に対応して時計を動作させることを特徴とする日時管理方法。

【０１２０】

（付記２２）複数の日時管理者からそれぞれ日時設定要求が入力されることができ、受け付けた日時設定要求に対応して日時を管理する計算機によって使用される記憶媒体において、

前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者からの日時設定要求を受け付けるステップと、

該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には、該あらかじめ定められた日時管理者からの日時設定要求だけを受け付けるステップと、

受け付けた日時設定要求に対応して時計を動作させるステップとを計算機に実行させるためのプログラムを格納した計算機読み出し可能可搬型記憶媒体。

【０１２１】

（付記２３）階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が

入力されることができ、受け付けた日時設定要求に対応して日時を管理するための計算機によって使用される記憶媒体において、

前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けるステップと、

該任意の日時管理者からの日時設定要求を受け付けた後には該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求だけを受け付けるステップと、

該受け付けた日時設定要求に対応して時計を動作させるステップとを計算機に実行させるプログラムを格納した計算機読み出し可能可搬型記憶媒体。

【０１２２】

（付記２４）複数の日時管理者からそれぞれ日時設定要求が入力されることのできる一般用日時管理装置と、該複数の日時管理者の側にそれぞれ備えられる管理者用日時管理装置とを有する日時管理システムにおいて、

前記一般用日時管理装置が、前記複数の日時管理者のうち、あらかじめ定められた日時管理者からの日時設定要求を受け付ける前には任意の日時管理者あからの日時設定要求を受け付け、該あらかじめ定められた日時管理者からの日時設定要求を受け付けた後には該定められた日時管理者からの日時設定要求だけを受け付ける日時設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段とを備えると共に、前記管理者用日時管理装置が、自装置が管理する日時の複写の要求を、前記日時設定要求として前記日時設定要求受付手段に与える日時設定要求手段を備えることを特徴とする日時管理システム。

【０１２３】

（付記２５）階層構造を持つ複数の日時管理者からそれぞれ日時設定要求が入力されることのできる一般用日時管理装置と、該複数の日時管理者の側にそれぞれ備えられる管理者用日時管理装置とを有する日時管理システムにおいて、

前記一般用日時管理装置が、前記複数の日時管理者のうち、任意の日時管理者からの日時設定要求を受け付けた後には、該任意の日時管理者よりも前記階層構造において上位の階層に属する日時管理者からの日時設定要求を受け付ける日時

設定要求受付手段と、

該受け付けられた日時設定要求に対応して動作する時計手段とを備えると共に、

前記管理者用日時管理装置が、自装置が管理する日時の複写の要求を、前記日時設定要求として前記日時設定要求受付手段に与える日時設定要求手段を備えることを特徴とする日時管理システム。

【０１２４】

【発明の効果】

以上詳細に説明したように、本発明によれば、例えばユーザ側の目的に応じた有効範囲内での日時管理、および時刻付き署名の機能を実現することが可能になる。日時管理装置や時刻付き署名装置の提供者側から見た場合にも、ユーザ毎に日時情報の設定などのカスタマイズを行う必要がなくなる。例えばユーザ側での日時情報や、署名の有効範囲の変更も、例えばユーザ側管理者によって自由に行うことができ、また逆に例えば国の日時管理センタのような機関からの日時情報設定を受けることによって、公的に有効な日時管理や時刻付き署名を実現することもでき、日時管理装置および時刻付き署名装置の実用性の向上に寄与するところが大きい。

【図面の簡単な説明】

【図１】

本発明の原理構成ブロック図である。

【図２】

日時管理装置における基本的な日時設定方式の説明図である。

【図３】

日時管理装置の階層構造の説明図である。

【図４】

時刻付き署名装置に対する日時情報設定と署名作成の基本方式の説明図である。

【図５】

時刻付き署名装置に対する日時管理の階層構造の説明図である。

【図６】

日時設定処理の基本フローチャートである。

【図７】

日時管理装置が階層構造を持つ場合の日時設定処理のフローチャートである。

【図８】

日時管理装置の運用例の説明図である。

【図９】

日時情報複写方式の詳細説明図である。

【図１０】

日時情報複写方式の他の例の説明図である。

【図１１】

日時管理装置内の時計の精度維持方式の説明図である。

【図１２】

時刻付き署名作成処理の全体フローチャートである。

【図１３】

時刻付き署名装置の処理フローチャートの他の例を示す図である。

【図１４】

時刻付き署名装置における署名作成の詳細説明図である。

【図１５】

ＤＥＳ－ＭＡＣ方式による署名作成の説明図である。

【図１６】

署名検証方式の説明図である。

【図１７】

時刻付き署名装置に対するパスワードリトライ回数と最低パスワード長の設定方式の説明図である。

【図１８】

パスワード更新処理のフローチャートである。

【図１９】

パスワードリトライ回数制限処理のフローチャートである。

【図２０】

本実施形態におけるプログラムのコンピュータへのローディングの説明図である。

【符号の説明】

１　日時管理装置

２，６　日時設定要求受付手段

３，７　時計手段

５　日時管理機能内蔵署名作成装置

８　署名作成手段

１０　ユーザ側日時管理装置

１１　日時管理者の日時管理装置

１２　特定の日時管理者の日時管理装置

１３，１５，１６　時計

１４　フラグ

２１～２５　日時管理装置

２６，２７　中間日時管理装置

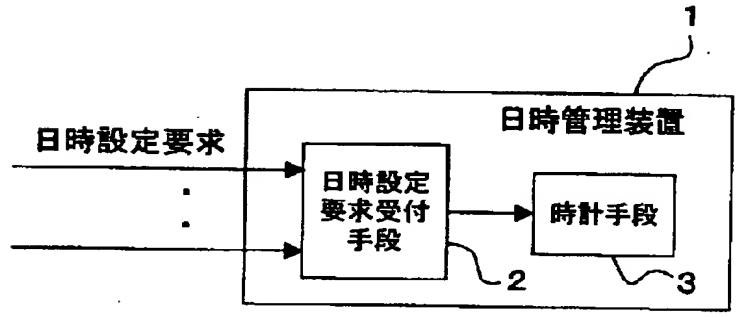
２８　最上位日時管理装置

４１～４５　時計付き署名装置

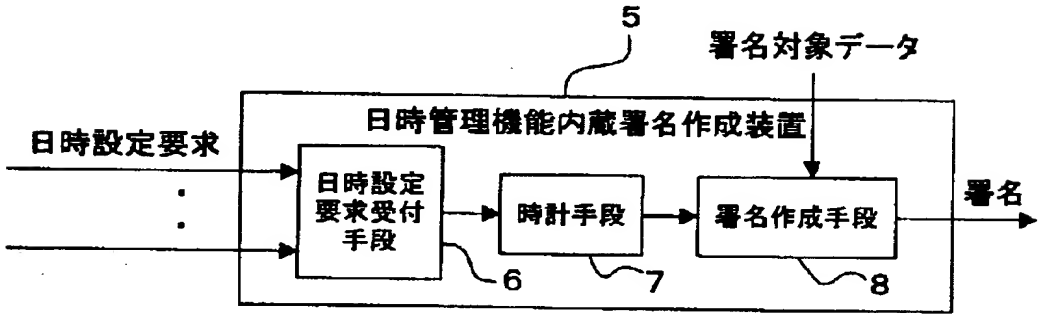
【書類名】　　図面

【図１】

本発明の原理構成ブロック図



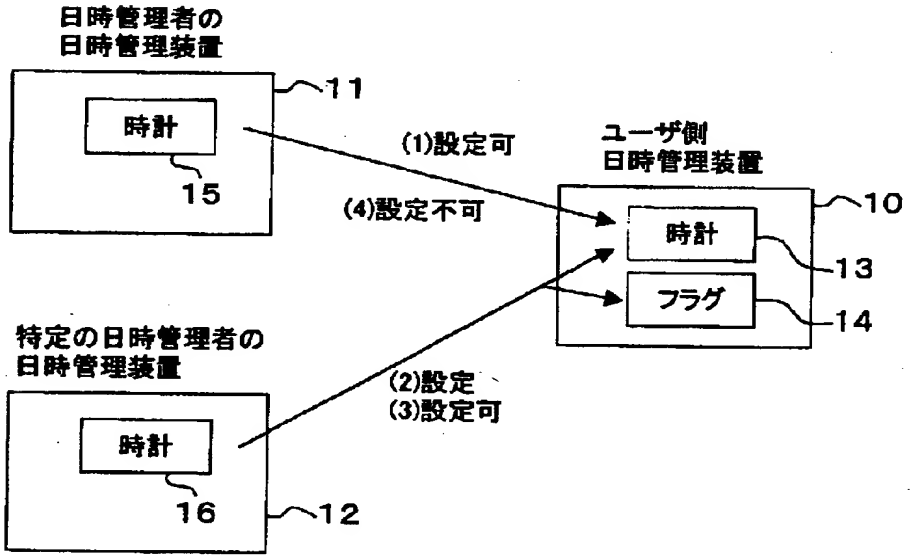
(a)



(b)

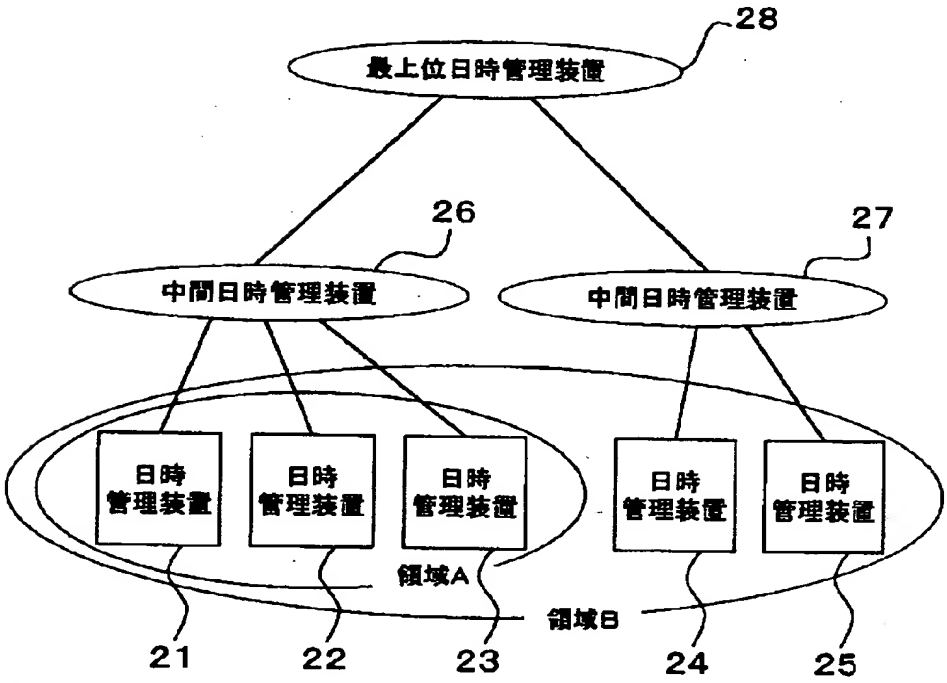
【図２】

日時管理装置における基本的な日時設定方式の説明図



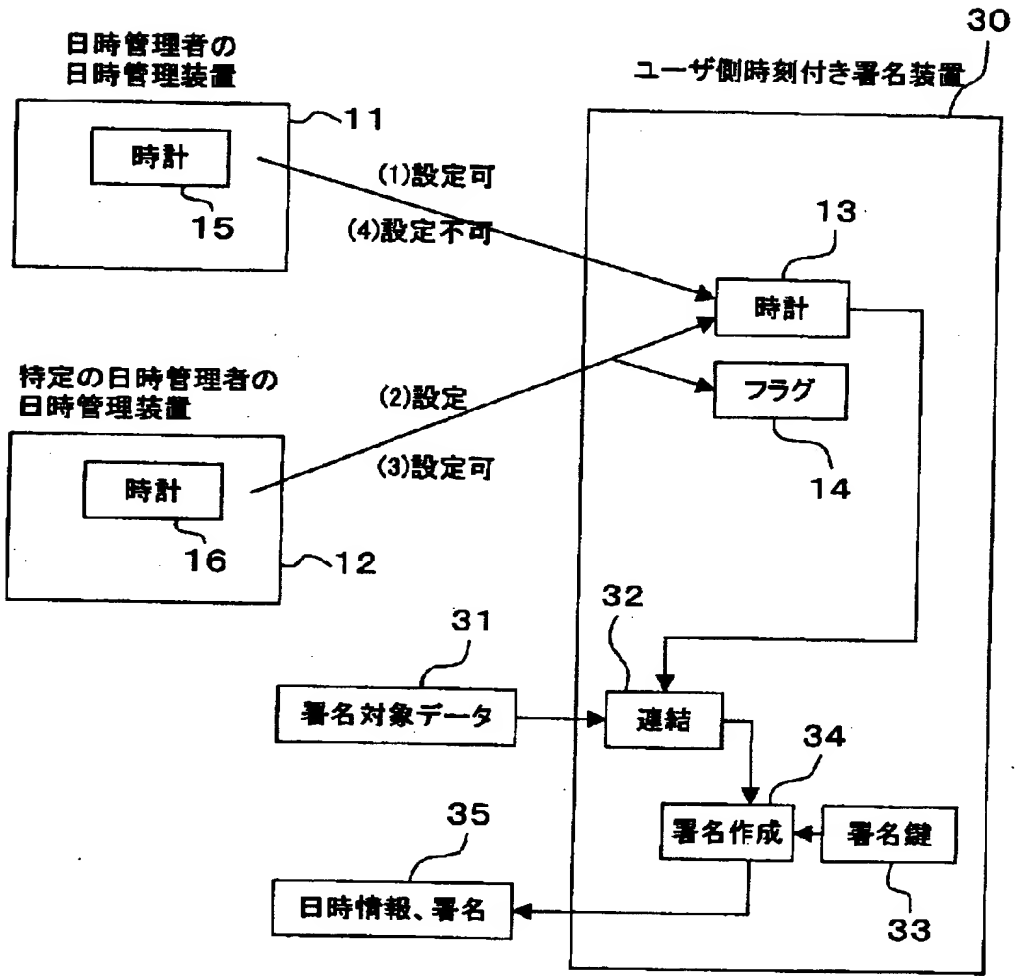
【図３】

日時管理装置の階層構造の説明図



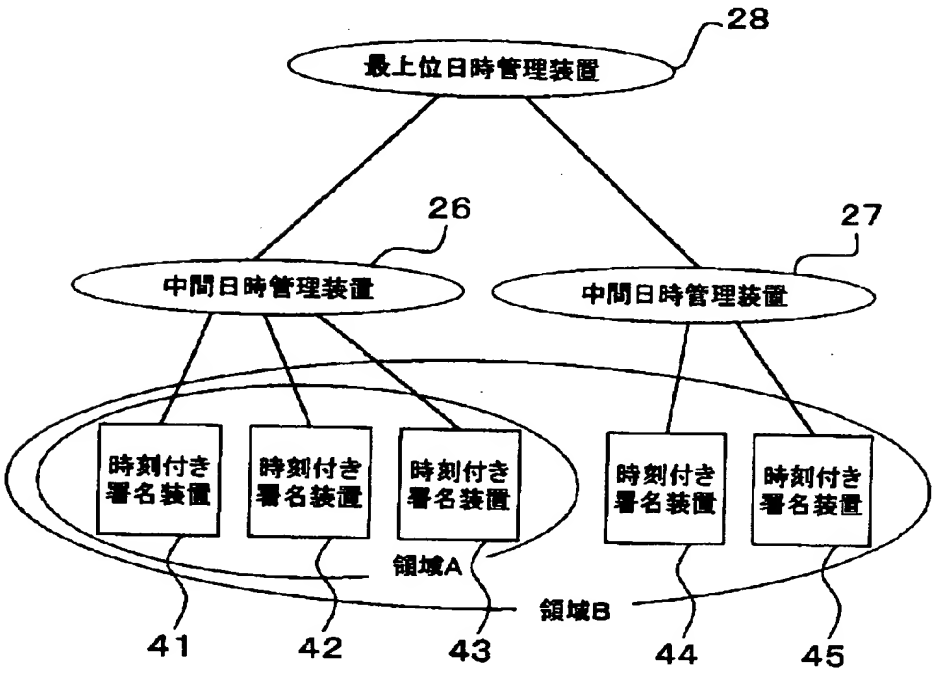
【図４】

時刻付き署名装置に対する日時情報設定と
署名作成の基本方式の説明図



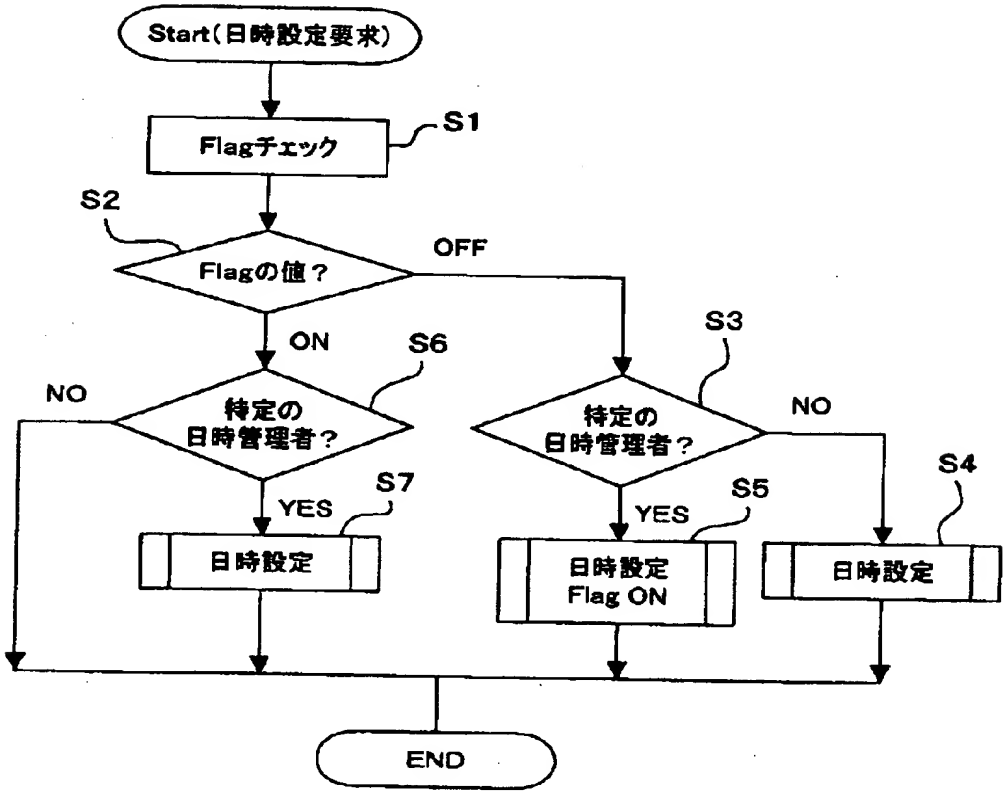
【図５】

時刻付き署名装置に対する
日時管理の階層構造の説明図



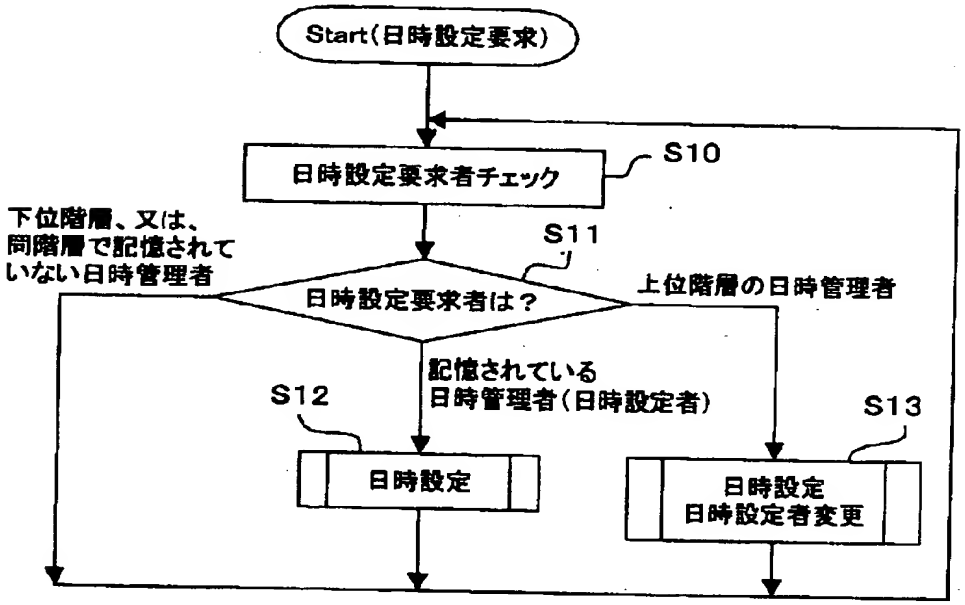
【図６】

日時設定処理の基本フローチャート



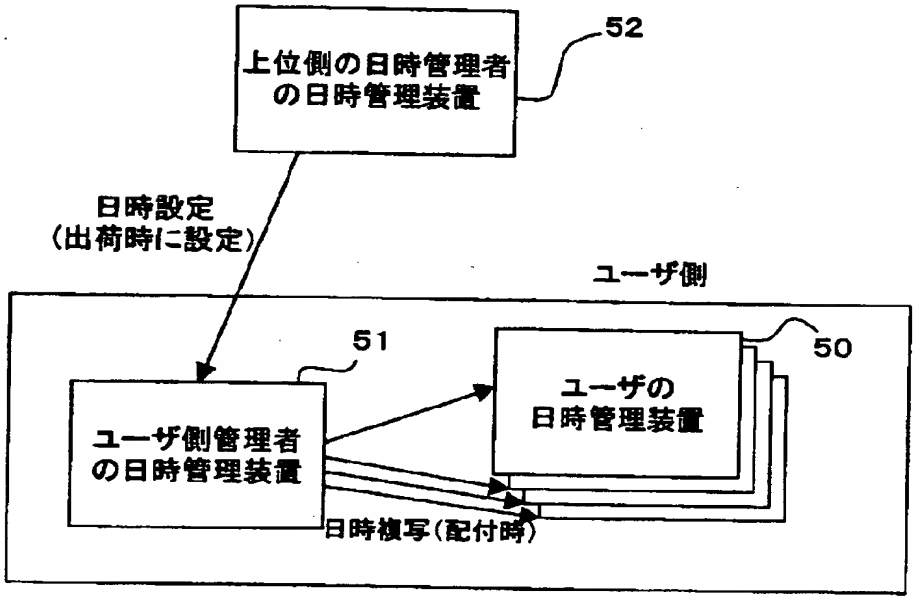
【図７】

日時管理装置が階層構造を持つ
場合の日時設定処理のフローチャート



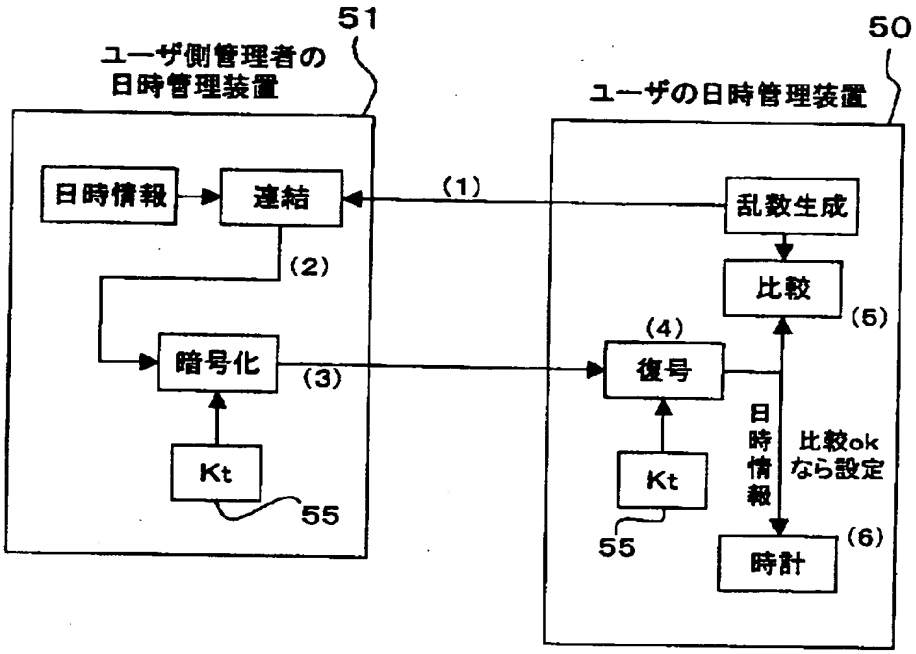
【図８】

日時管理装置の運用例の説明図



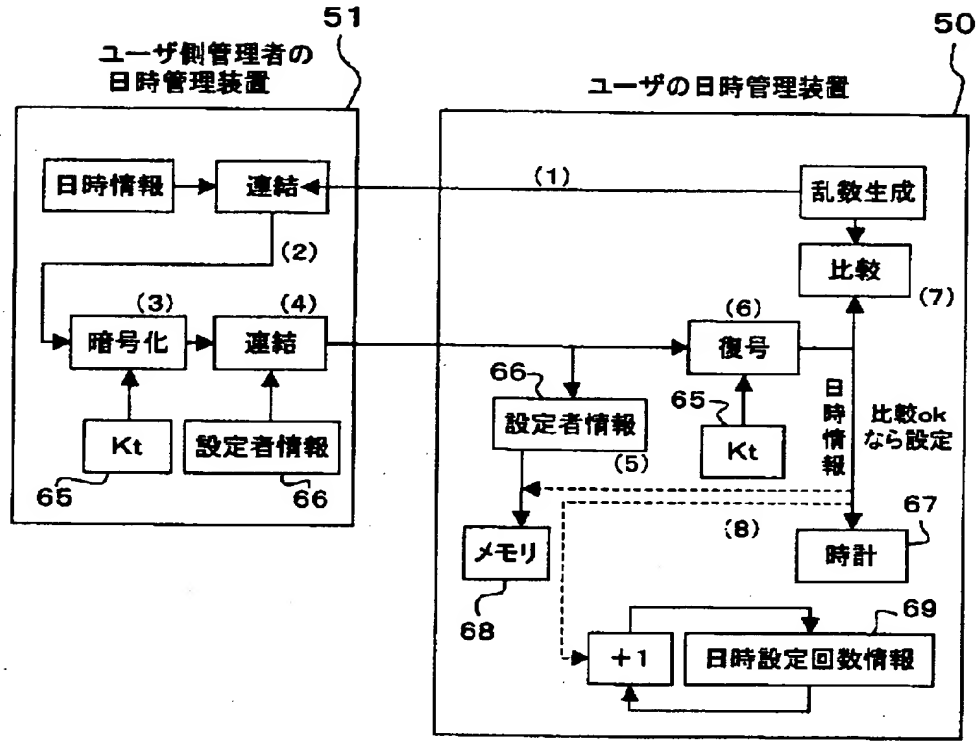
【図９】

日時情報複写方式の詳細説明図



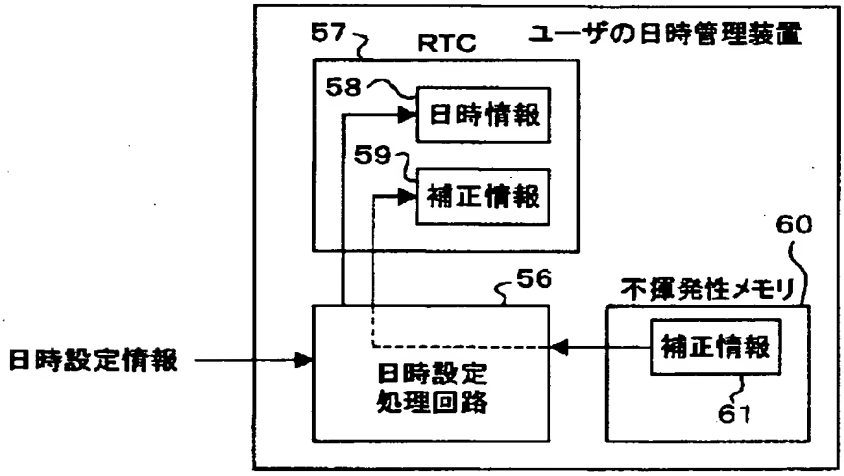
【図１０】

日時情報複写方式の他の例の説明図



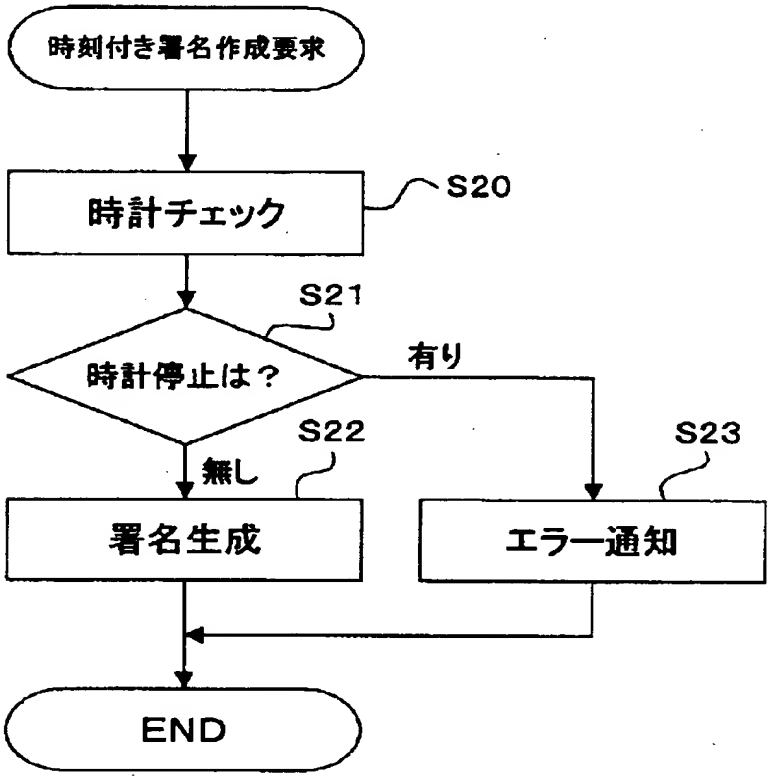
【図１１】

日時管理装置内に時計の精度維持方式に説明図



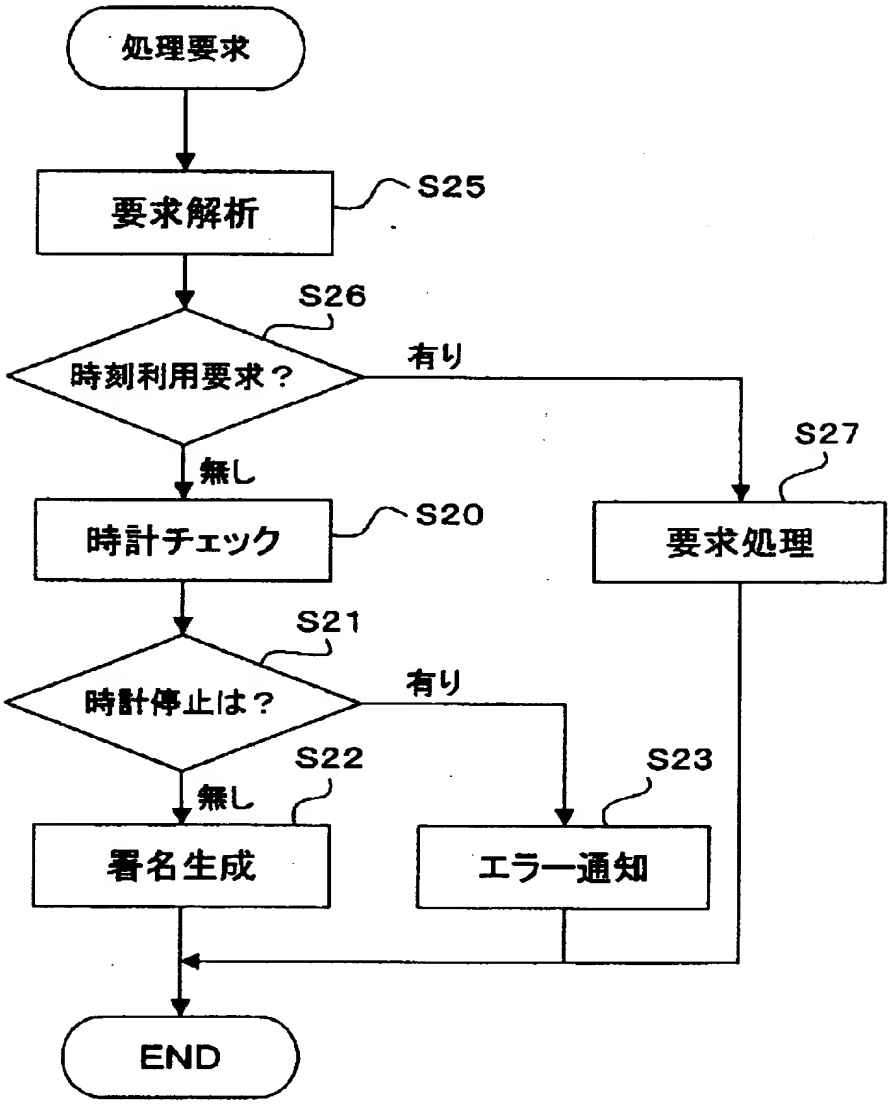
【図１２】

時刻付き署名作成処理の全体フローチャート



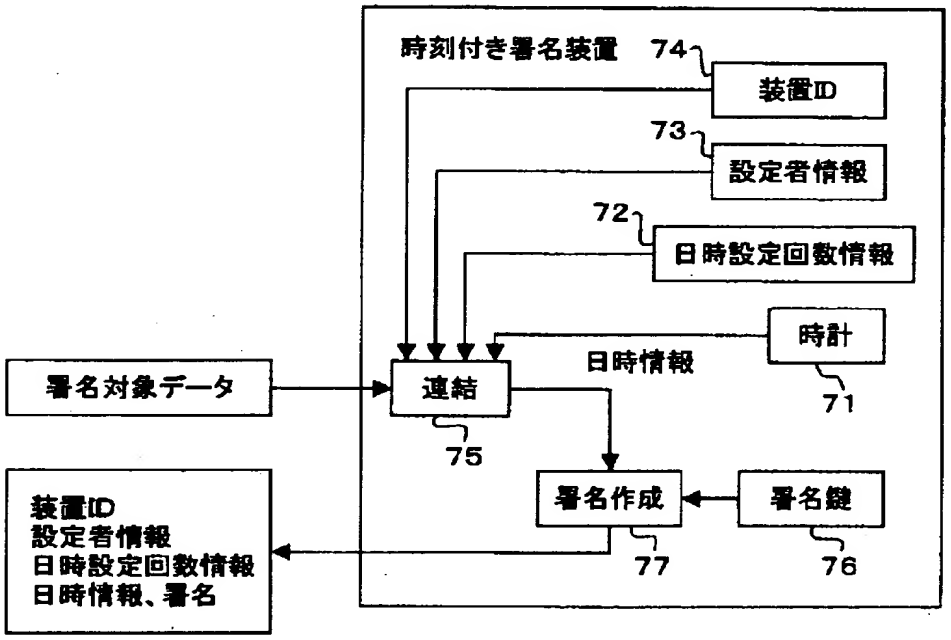
【図１３】

時刻付き署名装置の処理フローチャートの他の例を示す図



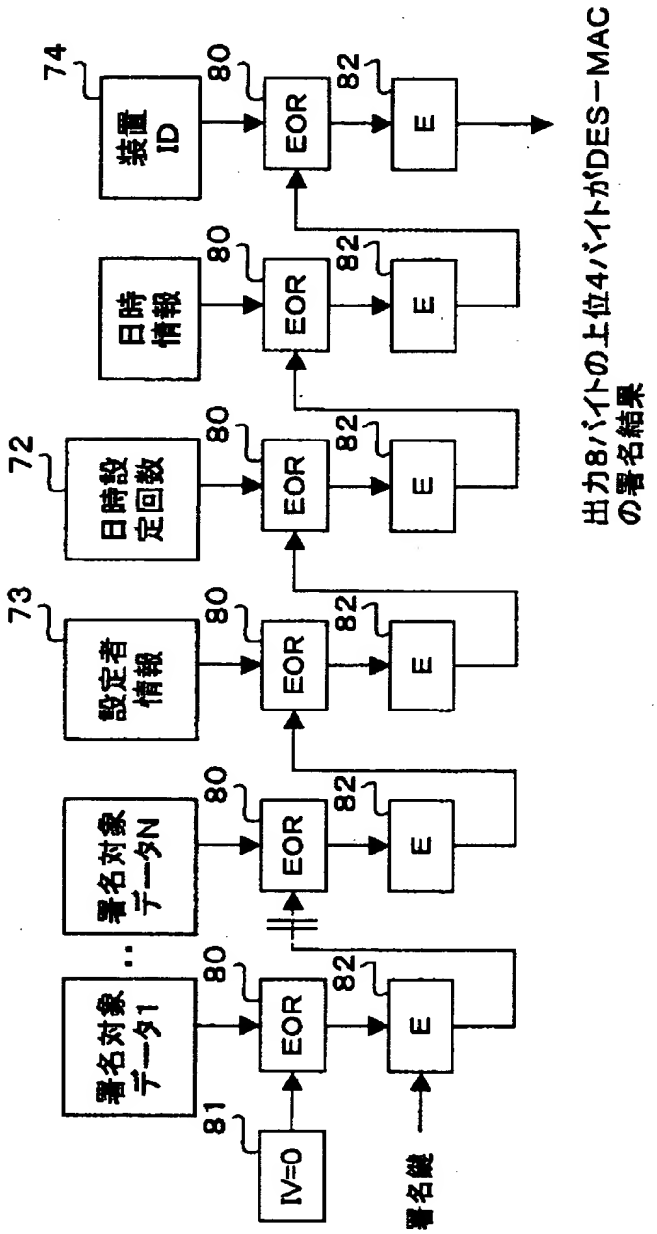
【図１４】

時刻付き署名装置における署名作成の詳細説明図



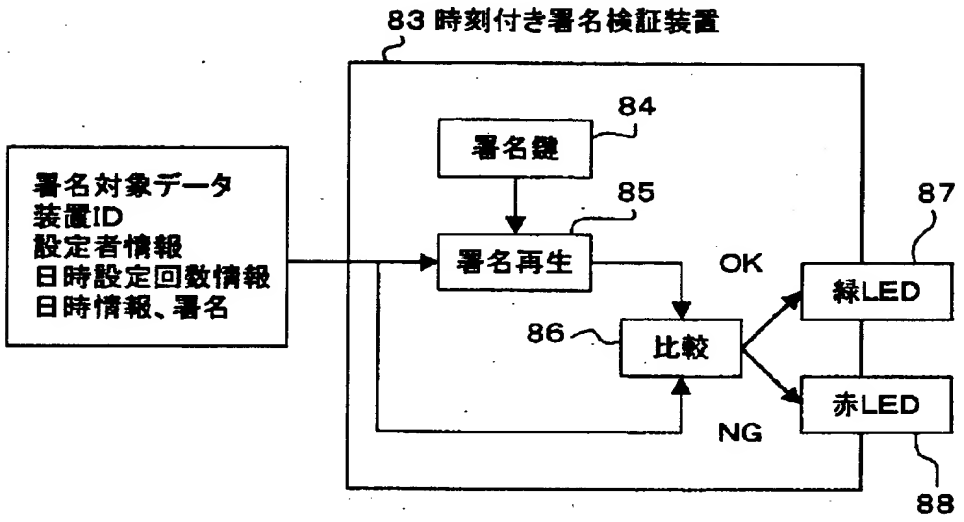
【図１５】

DES－MAC方式による署名作成の説明図



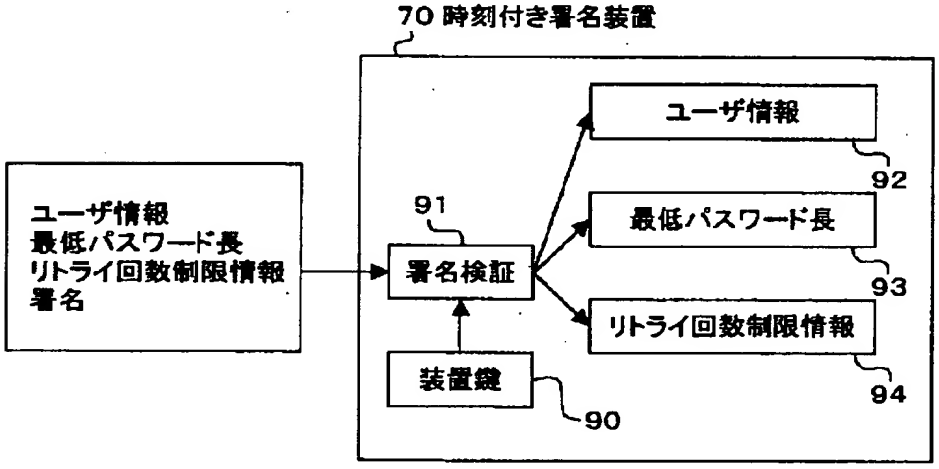
【図１６】

署名検証方式の説明図



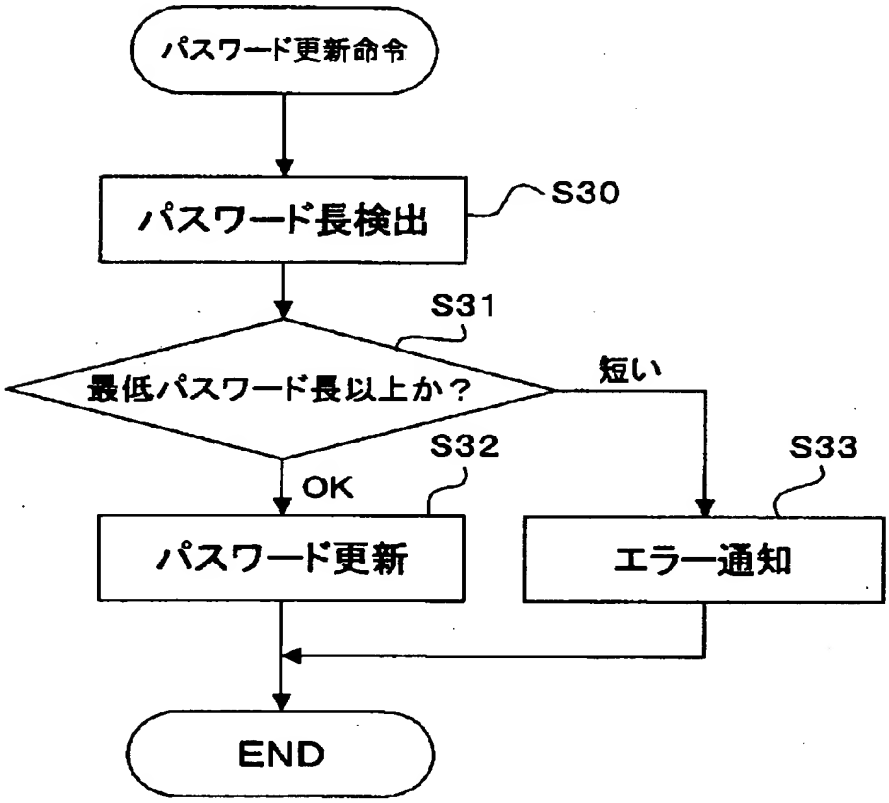
【図１７】

時刻付き署名装置に対するパスワードリトライ回数と最低パスワード長の設定方式の説明図



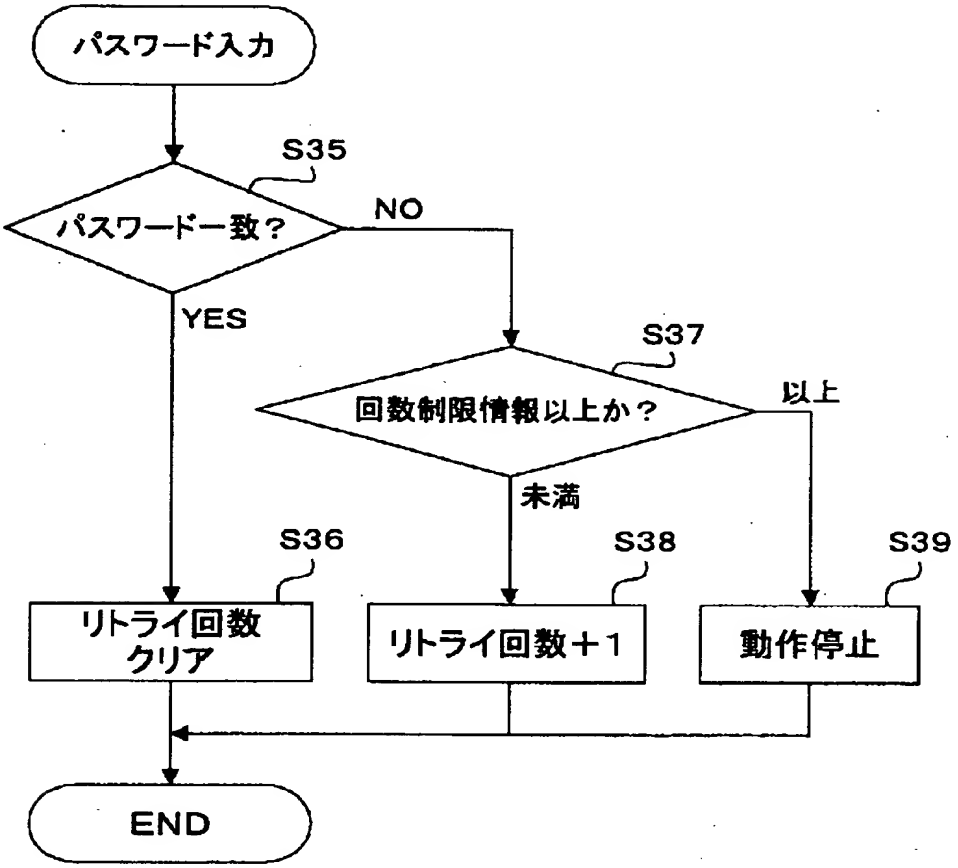
【図１８】

パスワード更新処理のフローチャート



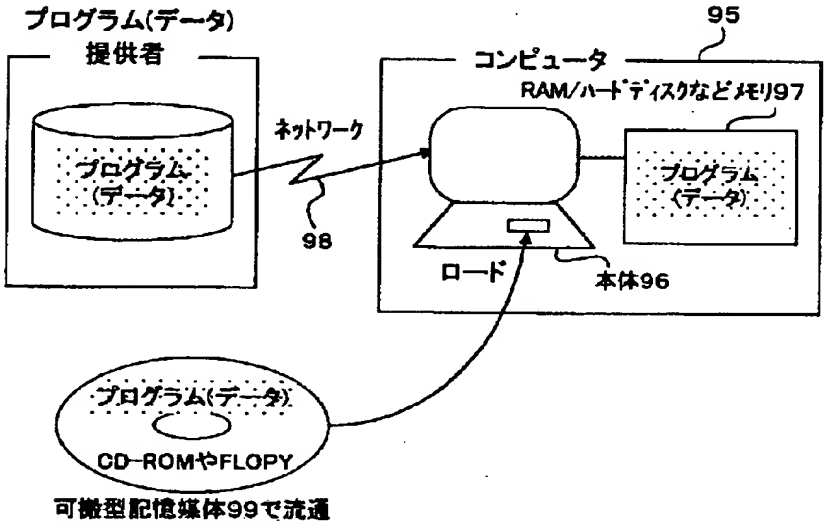
【図１９】

パスワードリトライ回数制限処理のフローチャート



【図２０】

本発明におけるプログラムの
コンピュータへのローディングを説明する図



【書類名】　　要約書

【要約】

【課題】　組織の内部のみで有効な日時管理を実現することも、また組織の外部でも有効な、例えば公的な日時管理を実現することも可能とする。

【解決手段】　それぞれ日時設定要求を出すことができる複数の日時管理者のうちで、あらかじめ定められた管理者からの設定要求を受け付ける前には任意の管理者からの設定要求を受け付け、定められた管理者からの設定要求を受け付けた後には該定められた管理者からの設定要求だけを受け付ける手段２と、受け付けられた日時設定要求に対応して動作する時計手段３とを備える。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社